View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 32 (2012) 536 – 543

Procedia Engineering

www.elsevier.com/locate/procedia

I-SEEC2011

Privacy Amplification of QKD Protocol in a Quantum Router

S. Chaiyasoonthorn[a] , P. Youplao[b*], S. Mitatha[b], P.P. Yupapin[c]

[a]*Department of Electronic Technology, Faculty of Science, Ramkhamhaeng University, Bangkok 10240, Thailand,*
[b]*Hibrid Computing Research Laboratory, Faculty of Engineering,*
[c]*Nanoscale Science and Engineering Research Alliance, Faculty of Science,*
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand

Elsevier use only: Received 30 September 2011; Revised 10 November 2011; Accepted 25 November 2011.

Abstract

We propose a new system of quantum cryptography for QKD protocol with privacy amplification for internet security using Gaussian pulse propagating within a nonlinear ring resonator system, quantum processor and a wavelength router. To increase the channel capacity and security, the multiplexer is operated incorporating a quantum processing unit via an optical multiplexer. The transmission part can be used to generate the high capacity quantum codes within the series of micro ring resonators and an add/drop filter. The receiver part can be communicated by using the quantum key (quantum bit, qubit) via a wavelength router and quantum processors. The reference states can be recognized by using the cloning unit, which is operated by the add/drop filter, where the communication between Alice and Bob can be performed. Results obtained have shown that the correlated photons can be generated and formed the entangled photon pair, which is allowed to form the secret key between Alice and Bob. In application, the embedded system within the computer processing unit is available for quantum computer.

© 2010 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of I-SEEC2011
Open access under CC BY-NC-ND license.

Keywords : Quantum protocol; Quantum network; QKD; Wavelength router; Dark soliton

1. Introduction

Demand of using internet has been increased widely and rapidly every year, therefore, the internet security becomes the important function which is required to include into the modern internet service. Up to date, a quantum technique is recommended to provide such a requirement. However, the security technique known as quantum cryptography has been widely used and investigated in many applications [1-3]. Recently, Suchat et al. [4] have reported the interesting concept of continuous variable quantum

* Corresponding author. *E-mail address*: phichai3112@yahoo.com.

1877-7058 © 2012 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2012.01.1305

key distribution via a simultaneous optical-wireless up-down-link system, where they have shown that the continuous variable quantum key could be performed via chaotic signals generated in a nonlinear micro-ring resonator system with appropriate soliton input power and micro-ring resonator parameters. They have also shown that the different time slot entangled photons can be formed randomly and can be used to select two different frequency bands for up-down-link converters within a single system. Yupapin et al [5] have proposed a new technique for QKD (Quantum Key Distribution) that can be used to make the communication transmission security and implemented with a small device such as mobile telephone hand set. This technique has proposed the Kerr nonlinear type of light in the micro ring resonator to generate the superposition of the chaotic signal via a four-wave mixing type that introduces the second-harmonic pulse. A technique used for communication security via quantum chaotic has been proposed by Yupapin and Chunpang [6], where the use of quantum-chaotic encoding of light traveling in a fiber ring resonator to generate two different codes i.e. quantum bits and chaotic signal is presented. Mitatha et al [7] have proposed the design of secured packet switching used nonlinear behaviors of light in micro ring resonator which can be made high-capacity and security switching. Such a system can also be used for the tunable band pass and band stop filters.

Ordinary computers process units of information called bits, which exist in one of two states: 1 or 0. Quantum computers would instead use units called “qubits” that can exist in either state, but also in both simultaneously. In the mysterious phenomenon of quantum entanglement, a measurement of a property of one particle guarantees that a particle "entangled" with it will have the same property, even if the two are far apart, in space. Shorter-range entanglement has been performed before, but the new study used a method of entanglement that in principle could be extended to any range, he went on. This “remote” entanglement is necessary for networks of quantum computers, he added, which would constitute a “quantum internet.” Very small-scale quantum computers have been claimed to work before, but physicists say large-scale ones that could effectively replace traditional computers are years away. By manipulating the photons emitted from each of the two atoms and guiding them to interact along a fiber optic thread, the researchers were able to entangle the atoms, Monroe said. While the thread was needed to establish entanglement, he added, the fiber could be severed and the atoms would stay entangled. In this paper, we have used a nonlinear micro ring resonator to form the correlated photons and quantum codes, where the secret key codes can be generated by using the entangled photon pair, which can be formed the secret key for two parties known as Alice and Bob by using the Gaussian light pulse propagating with the series of micro ring resonator. In application, the device can be embedded within the computer processing unit with using to increase the capacity and the speed for internet, where the internet security can be provided. However, the theoretical background of correlated photon source generation is reviewed.

2. Dense Wavelength Multiplexing Generation

Light from a monochromatic light source is launched into a ring resonator with constant light field amplitude (E_0) and random phase modulation as shown in Fig. 1, which is the combination of terms in attenuation (α) and phase (ω_0) constants, which results in temporal coherence degradation. Hence, the time dependent input light field (E_{in}), without pumping term, can be expressed as [8]. Where L is a propagation distance(waveguide length).

$$E_{in}(t) = E_0 e^{-\alpha L + j\phi_0(t)} \quad (1)$$

We assume that the nonlinearity of the optical ring resonator is of the Kerr-type, i.e., the refractive index is given by

$$n = n_0 + n_2 I = n_0 + n_2 \left(\frac{P}{A_{eff}} \right) \quad (2)$$

Where n_0 and n_2 are the linear and nonlinear refractive indexes, respectively. I and P are the optical intensity and optical power, respectively. The effective mode core area of the device is given by *Aeff*. For the microring and nanoring resonators, the effective mode core areas range from 0.10 to 0.50 μm2 [9]. When a Gaussian pulse is input and propagated within a fiber ring resonator, the resonant output is formed, thus, the normalized output of the light field is the ratio between the output and input fields in each roundtrip, which can be expressed as [10].

$$\left| \frac{E_{out}(t)}{E_{in}(t)} \right|^2 = (1-\gamma)\left[1 - \frac{(1-(1-\gamma)x^2)\kappa}{(1-x\sqrt{1-\gamma}\sqrt{1-\kappa})^2 + 4x\sqrt{1-\gamma}\sqrt{1-\kappa}\sin^2(\frac{\varphi}{2})} \right] \quad (3)$$

Eq. (3) indicates that a ring resonator in the particular case is very similar to a Fabry-Perot cavity, which has an input and output mirror with a field reflectivity, (1-κ), and a fully reflecting mirror. κ is the coupling coefficient, and $x = \exp(-\alpha L/2)$ represents a roundtrip loss coefficient, $\varphi_0 = kLn_0$ and $\varphi_{NL}=kL(n2/Aeff)P$ are the linear and nonlinear phase shifts, $k = 2\pi / \lambda$ is the wave propagation number in a vacuum. Where L and α are a waveguide length and linear absorption coefficient, respectively**.** In this work, the iterative method is introduced to obtain the results as shown in Eq. (3), similarly, when the output field is connected and input into the other ring resonators.

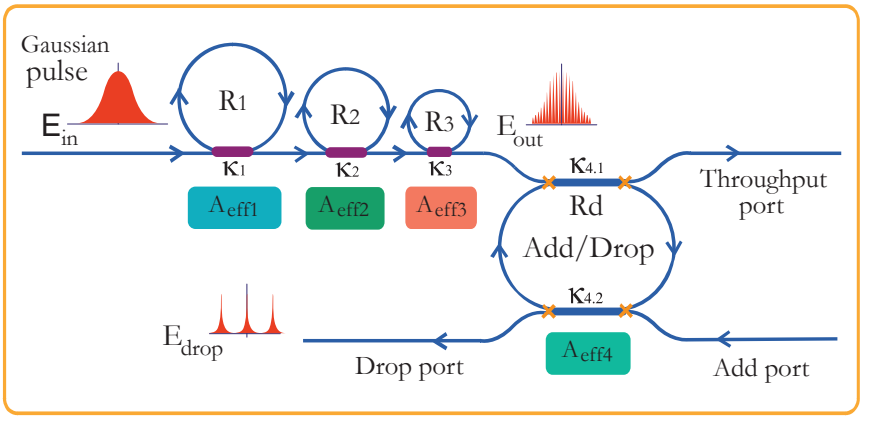

Fig. 1. A schematic of a Gaussian soliton generation system, where R_s: ring radii, κ_s: coupling coefficients, R_d: an add/drop ring radius, A_{effs}: Effective areas

The input optical field as shown in Eq. (1), i.e. a Gaussian pulse, is input into a nonlinear microring resonator. By using the appropriate parameters, the chaotic signal is obtained by using Eq. (3). To retrieve the signals from the chaotic noise, we propose to use the add/drop device with the appropriate parameters. This is given in details as followings. The optical outputs of a ring resonator add/drop filter can be given by the Eq. (4) and (5) [10, 11].

$$\left|\frac{E_t}{E_{in}}\right|^2 = \frac{(1-\kappa_{4.1})-2\sqrt{1-\kappa_{4.1}}\cdot\sqrt{1-\kappa_{4.2}}\,e^{-\frac{\alpha}{2}L}\cos(k_nL)+(1-\kappa_{4.2})e^{-\alpha L}}{1+(1-\kappa_{4.1})(1-\kappa_{4.2})e^{-\alpha L}-2\sqrt{1-\kappa_{4.1}}\cdot\sqrt{1-\kappa_{4.2}}\,e^{-\frac{\alpha}{2}L}\cos(k_nL)} \quad (4)$$

$$\left|\frac{E_d}{E_{in}}\right|^2 = \frac{\kappa_{4.1}\kappa_{4.2}e^{-\frac{\alpha}{2}L}}{1+(1-\kappa_{4.1})(1-\kappa_{4.2})e^{-\alpha L}-2\sqrt{1-\kappa_{4.1}}\cdot\sqrt{1-\kappa_{4.2}}\,e^{-\frac{\alpha}{2}L}\cos(k_nL)} \quad (5)$$

where E_t and E_d represents the optical fields of the throughput and drop ports respectively. The transmitted output can be controlled and obtained by choosing the suitable coupling ratio of the ring resonator, which is well derived and described by reference [11]. Where $\beta = kn_{eff}$ represents the propagation constant, n_{eff} is the effective refractive index of the waveguide, and the circumference of the ring is $L = 2\pi R$, here R is the radius of the ring. In the following, new parameters will be used for simplification, where $\varphi = \beta L$ is the phase constant. The chaotic noise cancellation can be managed by using the specific parameters of the add/drop device, which the required signals at the specific wavelength band can be filtered and retrieved. K_1 and K_2 are coupling coefficient of add/drop filters, $kn=2\pi / \lambda$ is the wave propagation number for in a vacuum, and the waveguide (ring resonator) loss is α = 0.5 dBmm-1. The fractional coupler intensity loss is $\gamma = 0.1$. In the case of add/drop device, the nonlinear refractive index is neglected.

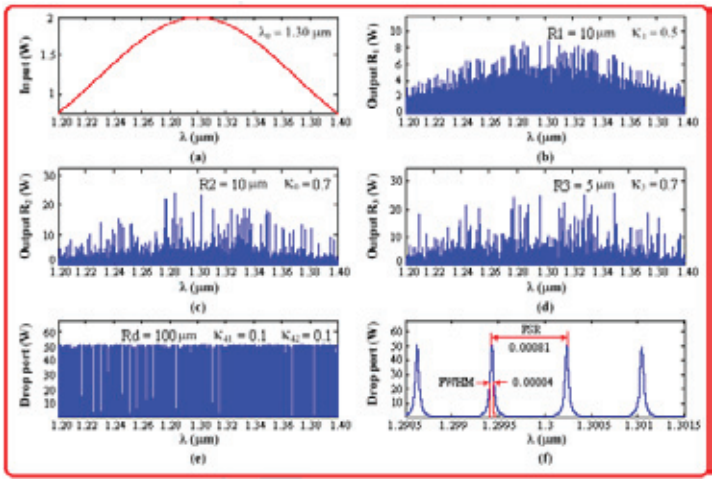

Fig. 2. Result of the spatial pulses with center wavelength at 1.30 μm, where (a) the Gaussian pulse, (b) large bandwidth signals, (c) and (d) large amplified signals, (e) and (f) filtering and amplifying signals from the drop port

From Fig. 1, in principle, light pulse is sliced to be the discrete signal and amplified within the first ring, where more signal amplification can be obtained by using the smaller ring device (second ring and third ring). Finally, the required signals can be obtained via a drop port of the add/drop filter. In operation, an optical field in the form of Gaussian pulse from a laser source at the specified center wavelength is input into the system. From Fig. 2, the Gaussian pulse with center wavelength (λ_0) at 1.30 μm, peak power at 2 W is input into the system as shown in Fig. 2(a). The large bandwidth signals can be seen within the first microring device, and shown in Fig. 2(b). The suitable ring parameters are used, for instance, ring radii R1 = 10 μm, R2 = 10 μm, R3 = 5.0 μm, and Rd = 25.0 μm. In order to make the

system associate with the practical device [12], the selected parameters of the system are fixed to n0 = 3.34 (InGaAsP/InP), Aeff = 0.50 μm2 and 0.25 μm2 for a microring, Aeff = 0.10 μm2 for a nanoring and add/drop ring resonator, respectively, α = 0.5 dBmm-1, γ = 0.1. In this investigation, the coupling coefficient (kappa, κ) of the microring resonator is ranged from 0.50 to 0.90. The nonlinear refractive index of the microring used is n2 = 2.2 x 10-17 m2/W. In this case, the attenuation of light propagates within the system (i.e. wave guided) used is 0.5 dBmm-1. After light is input into the system, the Gaussian pulse is chopped (sliced) into a smaller signal spreading over the spectrum due to the nonlinear effects[10], which is shown in Fig. 2(a). The large bandwidth signal is generated within the first ring device. In applications, the specific input or out wavelengths can be used and generated.

We have shown that the multi-wavelength bands can be generated by using a Gaussian pulse propagating within the microring resonator system, which is available for the extended DWDM with the wavelength center at 1.30 μm, which can be used with the existed public networks, where the nondispersive wavelength (1.30 μm) can be extended and used to increase the communication capacity, furthermore, for long distance link, the pumping is not required in such a system. Moreover, the problem of signal collision can be solved by using the suitable FSR design [11]. In general, by using the wider range of ring parameters, the spectral range of the output can be covered wider range instead of fraction of nm. The large increasing in peak power is seen when light propagates from the large to small effective core area, where the other parameter is the coupling coefficient. However, the amplified power is required to control to keep the device being realistic.

3. Quantum Router

From the results obtained as shown in Fig. 2, the quantum bits can be formed by using the pair of the entangled photons which can be generated by using the correlated photons via a quantum processor (QP) as shown in Fig. 3A and 3B, therefore, the synchronous data transmission with high security can be performed by using the proposed designed system. Generally, there are two pairs of possible polarization entangled photons forming within the ring device, which are represented by the four polarization orientation angles as [0º, 90º], [45º and 135º]. These can be formed by using the optical component called the polarization rotatable device and a polarizing beam splitter. This concept is well described by the published work [19].

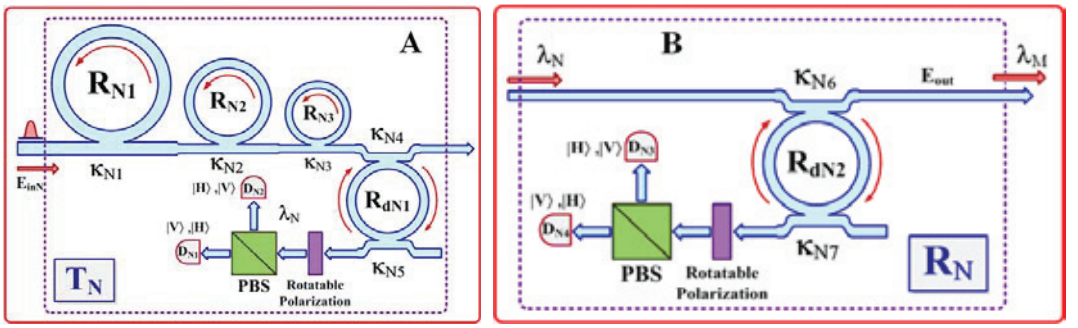

Fig. 3. A) system of Signal pulse and entangled photon generation, where R_{NS} : ring radii κ_{NS}: coupling coefficients, R_{dNS}: an add/drop ring radius, can be used to be the transmission part (T_N), B) system of the entangled photon pair manipulation of the receiver part (R_N). The quantum state is propagating to a rotatable polarizer and then is split by a beam splitter (PBS) flying to detector D_{N3} and D_{N4}

The remaining part of a system of the multi wavelength router is as shown in Fig. 4. In operation, the packet of data in each layer can be generated and input into the system via a wavelength router, which is

encoded by the quantum secret codes. The required data generated by specific wavelength can be retrieved via the drop port of the add/drop filter in the router, whereas the quantum secret codes can be specified between Alice and Bob. Moreover, the high capacity of data can be applied by using more wavelength carries which can be provided by the correlated photon generation. In general, the use of dark soliton array is required to form the high capacity packet switching, the synchronous data transmission is formed by using the qubits, whereas the additional advantageous is that the data security can be provided.

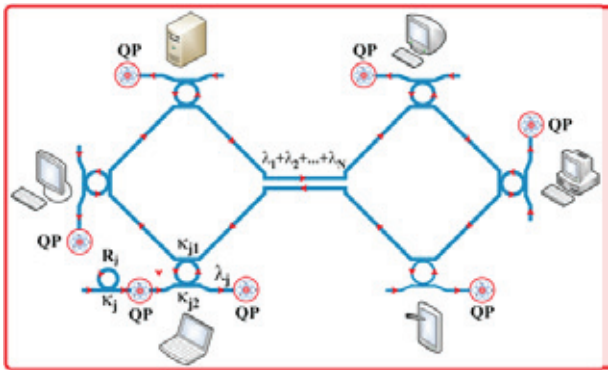

Fig. 4. A schematic multi wavelength router, where R_i, R_j: ring radii and κ_{is}, κ_{js} are the coupling coefficients, where λ_i: dark soliton wavelengths, QP: Quantum Processor

4. Proposed Protocol

Nowadays, there are many QKD protocol has been developing such as B92 protocol, EPR protocol, two-state protocol and others. The most widely used today is BB84 protocol. For this simulation, each of object (Alice, Bob, Eve) play different role. Only the appropriate function is executed on each of workstation, depends on its role. The quantum channel and public channel object are executed on Alice's, while Eve and Bob object are execute on different workstation respectively. In this work, we propose the use of multi layers QKD protocol which is similar to the ordinary QKD, but in this case there is more capacity which works as follow:

1)Alice generated a length (k) of random number (0 & 1) then sends it on Quantum channel object to be 'read' by Bob and Eve.

2)If there is eavesdropping from Eve, Eve is the one who have to 'read' the Quantum channel object first. Eve can modify the bits with two kind of attack; intercept/resend or beam splitting.

3)Then, Bob read the updated version from Quantum channel object, assuming that Bob doesn't know about the tapping from Eve.

4)Bob then measure the bits he 'read' from Quantum channel object with his selected own bases. Then, Bob 'announce' the bases he made to Alice via public channel, which located at Alice's.

5)Sifting raw key begin, Alice 'read' Bob's measurement at public channel object and confirm' to Bob the position Bob has measures in the right bases (m bits) by announce it at public channel.

6)Next, Alice and Bob estimate error to detect eavesdropper. They both calculate and compare their bits error rate (e). If they found that their error rate is higher than maximum bits error rate (e>emax), they will suspend the communication and start all over again. (emax has predetermined value)

7)Now, both Alice and Bob will have a shared key, which is called 'raw key'. This key is not really shared since Alice and Bob's version are different. They eliminate the m bits from the raw key.

8)Both Alice and Bob then perform 'error correction' on their raw key to find erroneous bits in uncompared parts of keys and 'privacy amplification' to minimize the number of bits that an eavesdropper knows in the final key.

9)Finally, they both will get a same string of bits, which is the shared secret key.

5. Privacy Amplification

The quantum key distribution protocols described above provide Alice and Bob with nearly identical shared keys, and also with an estimate of the discrepancy between the keys. These differences can be caused by eavesdropping, but also by imperfections in the transmission line and detectors. As it is impossible to distinguish between these two types of errors, guaranteed security requires the assumption that all errors are due to eavesdropping. Provided the error rate between the keys is lower than a certain threshold (about 20%) [20], two steps can be performed to first remove the erroneous bits and then reduce Eve's knowledge of the key to an arbitrary small value. These two steps are known as information reconciliation and privacy amplification respectively.

Privacy amplification uses Alice and Bob's key to produce a new, shorter key, in such a way that Eve has only negligible information about the new key. This can be done using a universal hash function, chosen at random from a publicly known set of such functions, which takes as its input a binary string of length equal to the key and outputs a binary string of a chosen shorter length. The amount by which this new key is shortened is calculated, based on how much information Eve could have gained about the old key, in order to reduce the probability of Eve having any knowledge of the new key to a very low value.

6. Conclusion

We have proposed a new technique of multi wavelength quantum key distribution via a wavelength router using the correlated photon. In this study, the multi wavelength signals are generated to form multivariable quantum key and packet switching data, which they are available for high capacity and security communication applications. In operation, the packet of data can be generated and input into the system via a wavelength router, which is encoded by the quantum secret codes. The advantage is that data identification can be transmitted associating with the information data, whereas the synchronous key can be provided between Alice and Bob by using the Gaussian pulse to form the quantum bits by using the correlated photons via the quantum processor. Initially, the Gaussian pulse is generated and used to form the multivariable packet switching data, where the sequence of data can be identified by quantum signals, whereas the security of data can be performed by using the secret codes. Moreover, the secret codes can also be used to form the data identification by using the parity bits which is known as signal synchronization. Finally, the required data generated by specific wavelength can be retrieved via the drop port of the add/drop filter in the wavelength router and the quantum secret codes can be specified between Alice and Bob.

Acknowledgements

The project was supported by Telecommunications Research and Industrial Development Institute (TRIDI), with National Telecommunication Commission of Thailand.

References

[1] P.P. Yupapin, W. Suwancharoen, “Entangled photon states generation and regeneration using a nonlinear fiber ring resonator”, Int. J. Light Electron. Opt., 120(15)(2009)746-751.

[2] P.P.Yupapin, “Generalized quantum key distribution via microring resonator for mobile telephone networks”, Int. J. Light Electron. Opt., (2008). doi:10.1016/j.ijleo.2008.07.030

[3] C. Sripakdee, P.P.Yupapin, “Quantum noise generated by four-wave mixing process with in a fiber ring resonator”, Int. J. Light Electron. Opt., (2009). doi:10.1016/j.ijleo.2008.12.021
[4] S. Suchat, N. Pornsuwancharoen and P.P Yupapin, “Continuous variable quantum key distribution via a simultaneous optical wireless up-down-link system”, Int. J. Light Electron. Opt., (2009). doi:10.1016/j.ijleo.2008.11.012.
[5] P.P. Yupapin, S. Thongme and K. Sarapat, “Second-harmonic generation via microring resonators for optimum entangled photon visibility”, Int. J. Light Electron. Opt., (2009). doi:10.1016/j.ijleo.2008.09.017
[6] P.P. Yupapin, P. Chunpang, “A quantum-chaotic encoding system using an erbium-doped fiber amplifier in a fiber ring resonator”, Int. J. Light Electron. Opt., 120(18)(2009)976-979.
[7] S. Mitatha, K. Dejhan, P.P. Yupapin and N. Pornsuwancharoen. “High-capacity and security packet switching using the nonlinear effects in microring resonators”, Int. J. Light Electron. Opt. (2008). doi:10.1016/j.ijleo.2009.03.012.
[8] D. Deng and Q. Guo, “Ince-Gaussian solitons in strongly nonlocal nonlinear media”, Opt. Lett., 32(2007)3206-3208.
[9] Q. Xu and M. Lipson, “All-optical logic based on silicon micro-ring resonators,” Opt. Exp. 15(3)(2007)924-929.
[10] P.P. Yupapin and W. Suwancharoen, “Chaotic signal generation and cancellation using a microring resonator incorporating an optical add/drop multiplexer,” Opt. Commun., 280(2)(2007)343-350.
[11] P.P. Yupapin, P. Saeung and C. Li, “Characteristics of complementary ring-resonator add/drop filters modeling by using graphical approach”, Opt. Commun., 272(2007)81-86.
[12] Y. Kokubun, Y. Hatakeyama, M. Ogata, S. Suzuki, and N. Zaizen, “Fabrication technologies for vertically coupled microring resonator with multilevel crossing busline and ultracompact-ring radius,” IEEE J. Sel. Top. Quantum Electron. 11, 4–10(2005).
[13] P.P. Yupapin and S. Suchat, “Entangle photon generation using fiber optic Mach-Zehnder interferometer incorporating nonlinear effect in a fiber ring resonator, Nanophotonics (JNP), 1, (2007)13504-1.
[14] H. Hubel1, M. R. Vanner, T. Lederer, B. Blauensteiner, T. Lorunser, A. Poppe1 and A. Zeilinger, “High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber”, Opt. Exp., 15(2007) 7853-7862.
[15] N. Pornsuwancharoen, P.P. Yupapin, “Entangled photon states recovery and cloning via the micro ring resonators and an add/drop multiplexer”, Int. J. Light and Electron Opt., doi:10.1016/j.ijleo.2008.09.034.
[16] K. Takada, M. Abe, T. Shibata, and K. Okamoto, “Field demonstration of over 1000-channel DWDM transmission with supercontinuum multi-carrier source”, Electron. Lett. 38(2002)572-573.
[17] K. Sarapat, J. Ali and P.P. Yupapin, “A novel storage and tunable light source generated by a soliton pulse in a micro ring resonator system for super dense wavelength division multiplexing use,” Micorw. and Opt. Technol. Lett., 51(12)(2009) 2948-2952.
[18] M. K. Smit, “Progress in AWG design and technology,” PROCEED OF WFOPC 2005: 4TH IEEE/LEOS WORKSHOP ON FIBRES AND OPTICAL PASSIVE COMPONENTS, (2005), p. 26.
[19] N. Pornsuwancharoen, P.P. Yupapin, “Entangled photon states recovery and cloning via the micro ring resonators and an add/drop multiplexer”, Int. J. Light and Electron Opt., doi:10.1016/j.ijleo.2008.09.034
[20] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate,” Optics Express, Vol. 16, Issue 23, pp. 18790-18979.